「量子コンピュータの登場に伴う機会とリスクに備えた計画に関する
G7 サイバー・エキスパート・グループによるステートメント」の仮訳

- サイバー・エキスパート・グループ（CEG）は、G7 の財務大臣及び中央銀行総裁に、金融システムの安全性と強靭性にとって重要なサイバーセキュリティに関する政策事項を助言している。G7 CEG は、量子コンピューティングには、金融システムに対する潜在的な便益とリスクの両面があると考えている。CEG は、メンバー法域に対し、量子コンピュータの開発状況をモニターすること、官民の関係者間の協力を促進すること、そして、量子コンピューティングが既存の暗号化手法に対してもたらしうる潜在的なリスクへの対処について検討を開始することを推奨する。

（量子コンピューティングと金融システム）

- 量子コンピュータは、既存のコンピュータでは現実的な時間で解くことができないような問題を解くことができることを期待して開発が進められている。金融機関は、市場取引や投資業務（リスク管理を含む）、内部管理、予測戦略の最適化において、量子技術による計算速度の向上という便益を享受し得る。また、量子コンピュータは、より効率的な決済や、保有ポートフォリオの動的最適化にも活用できるかもしれない。量子鍵配送のような技術は、組織のデジタル通信システムのサイバーリスクに対する安全性強化にも有益であろう[1]。金融機関は、こうした新しい量子コンピュータの利用にあたっては、その利用に伴う潜在的なリスクに対して事前に対策を講じておく必要がある。量子コンピュータの導入が進むことは、悪意ある主体が当該技術を不正に利用して金融システムにおけるシステミックリスクや組織内のリスクを顕現化させる可能性もある。

（公開鍵暗号に対するリスク）

- 現在、デジタル通信や IT システムは、暗号化することで安全性を確保している。複雑なアルゴリズムを用いることで、通信の秘匿性や安全性を確保し、当人の通信であることを保証している。しかし、脅威主体は将来、量子コンピュータの固有の特性を使用して、既存の暗号技術を支えている数学的問題

[1] 国際標準化機構（ISO）は、当局及び業界にガイダンスを提供するために、量子暗号鍵配布のセキュリティに関する標準を公開しており、次の Web サイトで入手できる。
ISO/IEC 23837-1:2023 - Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements

を解決し、セキュリティで保護された通信で使用している暗号化技術を無効にし、顧客情報を含む金融機関データに接し得る可能性がある。脅威主体は、大規模な量子コンピューティングが普及することを想定して、量子コンピュータの能力が向上し、広く利用できるようになった時点で復号化することを目的として、機密データを傍受するという、「HNDL 攻撃[2]」スキームを検討している可能性もある[3]。また、この攻撃スキームは、デジタル通信、IT システム、及びデータを保護する従来の暗号アルゴリズムに脅威を与え、将来的に脅威主体に機密データへのアクセスを提供する可能性がある。その結果、組織の評判及び顧客のプライバシーの完全性を損なう可能性がある。

（耐量子暗号の標準化）

- 耐量子暗号（Post-Quantum Cryptography＜PQC＞）は、暗号アルゴリズムにおいて量子コンピュータがもたらしうるリスクに対して耐性を有し、かつ、既存の通信プロトコルやネットワークと相互運用性がある暗号システムを開発することに焦点をあてた研究分野である[4]。PQC は、国家・国際的なレベルで官・民にわたっていくつか取り組みが進行中であり、とりわけ、セキュリティ及び相互運用性を図る観点から標準化が進められている。例えば、米国立標準技術研究所（NIST）は、量子コンピュータ及び既存のコンピュータの性能が向上することに伴って生じるリスクから既存のシステムを保護するための PQC 公開鍵アルゴリズムの開発研究に取り組んできた[5]。NIST は 2017 年に耐量子暗号アルゴリズムを定めるために公開コンペを行い、これにより新たな暗号化標準の基礎が形成されることが期待されていた。第 1 弾が 2024 年 8 月に公表された[6]。また、欧州ネットワーク情報セキュリティ庁（ENISA）は、PQC の標準化プロセスに関する諸法域での研究成果を公表し、NIST 及び国際標準化機構（ISO）等の組織での作業を中心に、標準化後の課題やプロトコルの推奨事項に関する報告書を発表した[7]。

  更なる国際協調によって、G7 法域間の規制上のギャップや齟齬が生じるリ

---

[2] ＜仮訳注＞「Harvest now, decrypt later」の略。量子コンピュータが将来広く利用可能となった際に不正アクセスすることを想定し、サイバー脅威主体が、今のうちから暗号化された機密情報を窃取しておくという攻撃形態。
[3] Project Leap: quantum-proofing the financial system (bis.org)
[4] Next steps in preparing for post-quantum cryptography - NCSC.GOV.UK
[5] Post-Quantum Cryptography | CSRC (nist.gov)
[6] NIST Releases First 3 Finalized Post-Quantum Encryption Standards
[7] Cryptography — ENISA (europa.eu)

スクを削減できる。世界経済フォーラムは、英国の金融行動監視機構（FCA）と協働で、量子セキュリティを調査しており、複数の金融当局の参加を得てグローバルな規制アプローチに係る報告書を公表した[8]。

（提言）

- 汎用性のある量子コンピュータ（又はハイブリッドコンピュータ）は今後 10 年以内に現実のものとなる可能性が高まっている。ただ、少なくとも初期段階の量子コンピュータ（又はハイブリッドコンピュータ）が既存の暗号技術を完全に凌駕するだけの能力を備えたものとなるかどうかは不確実である[9]。しかしながら、金融セクターにおける官民の主体（「金融主体」）が、量子コンピュータが現実のものとなることを見越してリスク耐性を高める取り組みを進めるには、相応の時間と投資が必要である。対応には長いリードタイムが求められる可能性を踏まえ、官民の各主体は、そうした脅威に対処するための準備をなるべく早く開始することを推奨する。

- 金融主体に対しては、この新たに生じるリスクに対処するために、以下の措置を推奨する。

  1. **量子コンピューティング、それに伴うリスク、及びそのリスクを軽減するための戦略について理解の向上を図ること。**金融主体は、量子コンピューティングのリスク、特に暗号解読のリスク、と潜在的な技術的解決策をより理解するために、ベンダーやサードパーティ、その他対象分野の専門家と検討することが考えられる。金融主体が重点的に取り組む論点としては、量子技術発展の時間軸、脅威動向の変化、並びに量子技術に耐性のある現状及び新興の技術や手法等が考えられる。金融主体は、時が経つに応じてこうした分野の動向変化を追いかけることを検討すべきである。

  2. **各主体の責任が及ぶ範囲における量子コンピューティングのリスクを評価すること。**金融主体は、企業であれ法域であれ、それぞれの責任の及ぶ範囲について、量子コンピューティングのリスクを深く理解するべきである。その目的は、金融主体が、この問題に対して注力すべき労力のレベルと、注力すべき分野を特定することにある。準備が整っている

[8] Quantum Security for the Financial Sector: Informing Global Regulatory Approaches | World Economic Forum (weforum.org)
[9] 2022 Quantum Threat Timeline Report - Global Risk Institute

金融主体は、リスクを軽減するための領域を特定し、優先順位を付けるために、自組織内及び依存している主要なサードパーティ内で使用している重要データと現在の暗号化技術について、一覧表の作成を開始すべきである。またその準備が整っていない他の金融主体は、詳細な分析を行う前に、各金融主体における情報技術の責任者や主要なサービス提供者と議論することから作業を開始することも考えられる。量子技術がより成熟する前に重要データの保護に関するリスク許容度を議論しておくことも考えられる。

3. **量子技術リスクを軽減するための計画を策定すること。**金融主体は、ガバナンス構造を確立し、主要な利害関係者とその役割及び責任を特定し、暗号技術に関連する量子コンピュータの導入計画に基づく主な対応のマイルストーンの策定を検討すべきである。これには、上記２で述べた金融主体及びそのサードパーティで用いている暗号技術の一覧表作成が含まれ得る。また、脆弱な暗号技術から耐量子暗号技術への整然とした移行計画も含まれ得る。カナダ政府は、金融主体が量子コンピュータの脅威に備えるのに役立つ、量子準備ガイドを策定した[10]。

- G7 CEG は、金融当局が、各法域内の企業や関連組織と緊密に連携し、耐量子技術へ移行することの重要性について啓蒙することを推奨する。G7 CEG は、G7 の法域及び基準設定主体間の相乗効果を活用しつつ、関与すべき優先順位の高い事項から金融システムにおける官民全ての利害関係者との対話の促進を図るために、引き続きこの量子コンピュータのトピックにコミットする。

以　　上

[10] Quantum-Readiness Best Practices